Math 127, ~~Mon Apr 18~~ Wed Apr 20

- Reading for today: 8.1–8.3.
- Reading for Mon Apr 25: 8.4–8.5.
- PS08 due **today**(-ish)
- PS09 outline due **Mon**(-ish).

Five Facts for Finite Fields

1. **Prime power:** The characteristic of a finite field must be a prime p, and its order must be $q = p^e$ for some $e \geq 1$.
2. **Orders of elements:** The multiplicative group of a finite field is cyclic; i.e., if F has q elements, $F^\times$ must contain at least one element of order $q - 1$. Moreover, every element of $F^\times$ must have order dividing $q - 1$.
3. **Magic polynomial:** If F is a field of order q, then every $\alpha \in F$ is a root of $x^q - x$, or in other words, $\alpha^q = \alpha$ for every $\alpha \in F$. Consequently, $x^q - x$ factors as the product of all $(x - \beta)$, where β runs over all elements of F.
4. **Construction:** Every finite field of characteristic p is isomorphic to $\mathbf{F}_p[x]/(m(x))$ for some irreducible polynomial $m(x)$.
5. **Classification:** For any prime p and $q = p^e$ $(e \geq 1)$, there exists a field $\mathbf{F}_q$ of order q that is unique up to isomorphism.

Example: Some orders of elements in $\mathbf{F}_{64}$

Let $\mathbf{F}_{64} = \mathbf{F}_2[\alpha]$, where α is a root of $m(x) = x^6 + x + 1$. Show that α is a primitive element of $\mathbf{F}_{64}$, and find (some) orders of elements in $\mathbf{F}_{64}$.

$|F_{64}| = 64, |F_{64}^\times| = 63$ $\quad +1 = -1$

α root of $m(x)$: $\alpha^6 + \alpha + 1 = 0$

$\Rightarrow \alpha^6 = \alpha + 1 \Rightarrow$ reduced elts of F_{64}

$= \{$ pols in α deg $\leq 5 \}$

Show α prim

$\text{ord}(\alpha)$ div $63 \Rightarrow 1, 3, 7, 9, 21, 63$

$\alpha^1 = \alpha$

$\alpha^2 = \alpha^2$

$\alpha^3 = \alpha^3$

$\alpha^4 = \alpha^4$

$\alpha^5 = \alpha^5$

$\alpha^6 = \alpha + 1$

$\alpha^7 = \alpha^2 + \alpha$

not 1, 3, 7

$\alpha^8 = \alpha^3 + \alpha^2$

$\alpha^9 = \alpha^4 + \alpha^3$ not 9

$\alpha^{10} = \alpha^5 + \alpha^4$

$\alpha^{11} = \alpha^6 + \alpha^5 = \alpha^5 + \alpha + 1$

$\alpha^{12} = \alpha^6 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha$

$= \alpha^2 + 1$

$\alpha^{13} = \alpha^3 + \alpha$

$\alpha^{14} = \alpha^4 + \alpha^2$

$\alpha^{15} = \alpha^5 + \alpha^3$

$\alpha^{16} = \alpha^6 + \alpha^4 = \alpha^4 + \alpha + 1$

$\alpha^{17} =$ --

$\alpha^6 = \alpha + 1$

etc. $\alpha^{21} \neq 1$ so $ord(\alpha) = 63$

α prim

$ord(\alpha^4 + \alpha^3) = ord(\alpha^9)$

$ord(\alpha^9) = \frac{63}{gcd(9,63)} = \frac{63}{9} = 7$

Qs on PS08?

7.5.10 Prove $\mathbb{Z}[\alpha] \neq \mathbb{F}_q$.

$\mathbb{F}_q$ field w/ q elts

→ every nonzero elt is a unit

→ α unit: $\exists \beta \in \mathbb{F}_q$ st. $\alpha\beta = 1$

Building better codes (review)

- An $[n, k, d]$ code $\mathcal{C}$ is a binary linear code of **length** n, **dimension** k, and **minimum distance** d. In other words, $\mathcal{C}$ is a subspace of $\mathbf{F}_2^n$, $\dim \mathcal{C} = k$ as a subspace of $\mathbf{F}_2^n$, and the smallest nubmer of 1s appearing in a nonzero codeword of $\mathcal{C}$ is d.
- We would like k/n to be as large as possible, because k/n represents the portion of each transmitted message that contains useful data.
- Also, since the maximum number of errors that can be corrected in a single transmitted codeword is $\left\lfloor \frac{d-1}{2} \right\rfloor$, we would like d to be as large as possible.

It follows that to create a good code, we need to find $[n, k, d]$ codes where both k and d are as large as possible, given n.

Example: Longer Hamming codes

For an integer $r \geq 2$, let $n = 2^r - 1$, and let H_n be the $k \times n$ matrix whose ith column ($1 \leq i \leq n$) is the binary digits of the integer i, e.g., for $r = 3$ and $r = 4$:

$$H_7 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad \mathcal{H}_7 = \mathrm{Null}(H_7)$$

$$H_{15} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

The **Hamming n-code** $\mathcal{H}_n$ has parity check matrix H_n.

Theorem

For an integer $r \geq 2$ and $n = 2^r - 1$, the Hamming n-code $\mathcal{H}_n$ is an $[n, n - r, 3]$ code (so we can correct 1 error per transmission).

As $r \to \infty$, transmit almost 100% data, but can't correct much.

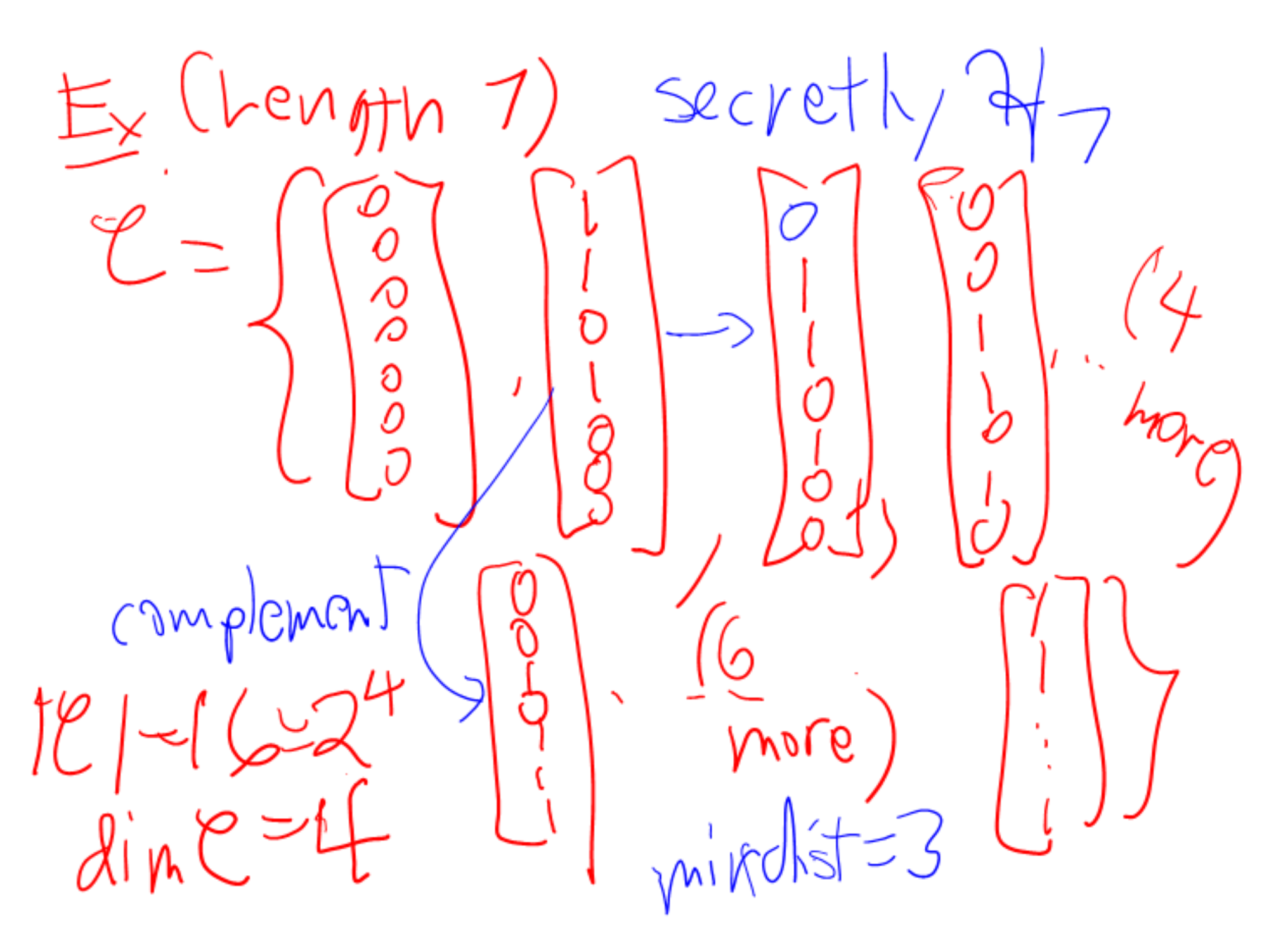
Cyclic codes

Definition

Let $\mathcal{C}$ be a binary linear code of length n. To say that $\mathcal{C}$ is **cyclic** means that it is closed under cyclic permutation of coordinates.

That is, to say that $\mathcal{C}$ is cyclic means that if $\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{bmatrix}$ is in $\mathcal{C}$, then

so are $\begin{bmatrix} c_{n-1} \\ c_0 \\ c_1 \\ \vdots \\ c_{n-2} \end{bmatrix}$, $\begin{bmatrix} c_{n-2} \\ c_{n-1} \\ c_0 \\ \vdots \\ c_{n-3} \end{bmatrix}$, and so on.


Ex (length 7)
secret, 7-7
C =
(4 more)
complement
(6 more)
|C| = 16 = 2^4
dim C = 4
min dist = 3

Polynomial notation: What is $xc(x)$?

The **polynomial notation** for vectors in $\mathbf{F}_2^n$ represents $\begin{bmatrix} c_0 \\ \vdots \\ c_{n-1} \end{bmatrix}$ as

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$$

in the ring $R = \mathbf{F}_2[x]/(x^n - 1)$ (i.e., setting $x^n = 1$).

If $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$, then in $\mathbf{F}_2[x]/(x^n - 1)$, we have:

$xc(x) = c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1} + c_{n-1} x^n$

$= c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1} + c_{n-1}$

$= c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1}$

$\mathbf{F}_2^n$ = polys of deg $\leq n-1$

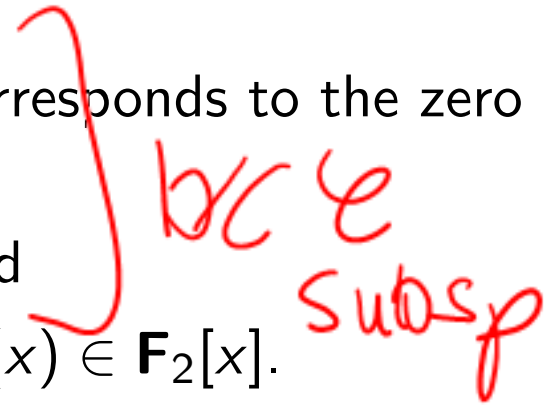
In vector form:

i.e. $xc(x)$ is cyclic rotation of orig vector $c(x)$.

Cyclic codes are ideals

Extrapolating that same idea (see PS09), suppose $\mathcal{C}$ is a cyclic code. Then:

- $\mathcal{C}$ contains the zero polynomial, which corresponds to the zero vector;
- $\mathcal{C}$ is closed under polynomial addition; and
- $\mathcal{C}$ is closed under multiplication by any $f(x) \in \mathbf{F}_2[x]$.



But we have a name for that kind of subset of $\mathbf{F}_2[x]$.
That's called an **ideal**. (!!!!)

Theorem

Let $\mathcal{C}$ be a binary linear code of length n. In polynomial notation, $\mathcal{C}$ is cyclic if and only if it is an ideal of the ring $\mathbf{F}_2[x]/(x^n - 1)$.

Proof: PS09.

The generator polynomial of a cyclic code

Theorem

Fix a positive integer n, and let $\mathcal{C}$ be a nonzero cyclic code of length n, i.e., let $\mathcal{C}$ be a nonzero ideal of $\overline{R} = \mathbf{F}_2[x]/(x^n - 1)$. Then $\mathcal{C}$ is principal, or in other words, $\mathcal{C} = (g(x))$ for some $g(x) \in \mathbf{F}_2[x]$. Moreover, we can choose $g(x)$ so that $g(x)$ divides $x^n - 1$.

Why: Can show that $\mathcal{C}$ comes from an ideal I of $\mathbf{F}_2[x]$. $\mathbf{F}_2[x]$ is a principal ideal domain (!!), so $I = (g(x))$ where $g(x)$ is the minimal polynomial of I. By taking gcds, we can take $g(x)$ to be a divisor of $x^n - 1$.

Point: Cyclic codes length n = divisors of $x^n - 1$

Definition

Let $\mathcal{C}$ be a cyclic code of length n. We define the **generator polynomial** of $\mathcal{C}$ to be the minimal polynomial $g(x)$ of $\mathcal{C}$.

The generator matrix of a cyclic code

Theorem

Let $\mathcal{C}$ be a cyclic code of length n generated by the divisor $g(x) \in \mathbf{F}_2[x]$ of $x^n - 1$. If $\deg g(x) = r$, then the set

$$\mathcal{B} = \left\{ g(x), xg(x), \ldots, x^{(n-1)-r} g(x) \right\}$$

len dcg

is a basis for $\mathcal{C}$. Consequently, the dimension of $\mathcal{C}$ is $k = n - r$.

Example: Let $\mathcal{C}$ be the cyclic code of length 6 generated by $(1 + x)$, which divides $x^6 - 1$ (since $-1 = +1$). The theorem says:

Generator matrix of a cyclic code (proof)

Linear indepedence: Generalizes the $(1 + x)$ example:

Spanning: See PS09.

The Hamming 7-code as a cyclic code

Consider the cyclic code of length 7 with generator polynomial $1 + x + x^3$.

Generators of cyclic codes: The upshot

Suppose $g(x)$ divides $x^n - 1$ in $\mathbf{F}_2[x]$. Let $\overline{R} = \mathbf{F}_2[x]/(x^n - 1)$.

- The principal ideal of $\overline{R}$ generated by $g(x)$ defines a cyclic code $\mathcal{C}$ of length n.
- The set $\left\{g(x), xg(x), \ldots, x^{(n-1)-r}g(x)\right\}$ is a basis for $\mathcal{C}$, and so the dimension of $\mathcal{C}$ is $k = n - r$.

Note: Coding and reading correctly received codewords can be done using polynomial multiplication and division, so we'll concentrate on being able to correct errors in principle (i.e., because of having a large minimum distance).

Big and difficult question: How can we compute the minimum distance of a cyclic code $\mathcal{C}$? Or at least, how can we ensure some kind of lower bound for the minimum distance of $\mathcal{C}$?

Extension fields

Definition

An **extension** of a field F is a field E that contains F as a subfield. A **finite extension** of a finite field $\mathbf{F}_q$ is an extension E of $\mathbf{F}_q$ such that E itself is a finite field.

Key example: If E is a finite field of characteristic 2, then one of the Five Facts for Finite Fields says that E contains $\mathbf{F}_2$ as a subfield. So E is a finite extension of $\mathbf{F}_2$.

Factoring over E vs. over $\mathbf{F}_2$

Definition

Let E be an extension of the field F, and suppose $f(x) \in F[x]$. To say that $f(x)$ **factors over** F means $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$, and to say that $f(x)$ **factors over** E means $f(x) = g(x)h(x)$ with $g(x), h(x) \in E[x]$. **Irreducible over** F and **irreducible over** E are defined similarly.

Example

The polynomial $x^3 + x + 1$ is irreducible over $\mathbf{F}_2$, but if α is a root of $x^3 + x + 1$ in $\mathbf{F}_8$, then

$$x^3 + x + 1 = (x - \alpha)(x - \alpha^2)(x - \alpha^4).$$

The BCH Theorem

Let $\mathcal{C}$ be a cyclic code of length n generated by the divisor $g(x) \in \mathbf{F}_2[x]$ of $x^n - 1$.
Suppose E is an extension of $\mathbf{F}_2$ such that for some $\delta \in \mathbf{N}$ and some $\alpha \in E$ with the order of α exactly equal to n, we have that

$$0 = g(\alpha) = g(\alpha^2) = g(\alpha^3) = \cdots = g(\alpha^{\delta-1}).$$

Then the minimum distance d of $\mathcal{C}$ is at least δ, i.e., $d \geq \delta$.

Example: $n = 7$, $g(x) = x^3 + x + 1$.